CLAIMS

By this response, no claims are amended, added, or canceled. For the Examiner's convenience, a copy of all pending claims and a status of the claims is provided below.

1. (previously presented) A method for checking network perimeter security, said method comprising the steps of:

reviewing security of a network perimeter architecture;

reviewing security of data processing devices that transfer data across the perimeter of the network;

reviewing security of applications that transfer data across said perimeter;

reviewing vulnerability of applications or data processing devices within said perimeter from computers or users outside of said perimeter; and

generating a report concerning security of said perimeter based upon all of the reviewing steps.

2. (original) The method as set forth in claim 1 further comprising the step of reviewing security of data processing devices within said perimeter that authenticate computers or users outside of said perimeter that request to access an application within said perimeter.

3. (original) The method as set forth in claim 1 further comprising the step of reviewing security of data processing devices that authorize computers or users outside of said perimeter that request to access an application within said perimeter.

4. (original) The method as set forth in claim 1 wherein the step of reviewing security of said data processing devices comprises the step of reviewing security of a web server, an e-mail server or an FTP server.

5. (original) The method as set forth in claim 1 further comprising the step of reviewing security of a server within said perimeter that provides data to said data processing devices that transfer data across the perimeter of said network.

6. (original) The method as set forth in claim 1 wherein each of said reviews is performed by comparison to a security policy of an enterprise which owns or controls said network.

7. (original) The method as set forth in claim 1 further comprising the step of determining said network perimeter.

8. (original) The method as set forth in claim 7 wherein said network perimeter comprises entries and exits from said network.

9. (original) The method as set forth in claim 1 wherein said network perimeter comprises entries and exits from said network.

10. (original) The method as set forth in claim 1 wherein the steps of reviewing security of a network perimeter architecture, reviewing security of data processing devices that transfer data across the perimeter of the network, and reviewing vulnerability of applications or data

processing devices within said perimeter from entities outside of said perimeter are performed at least in part with a respective program tool.

11. (original) The method as set forth in claim 1 wherein the step of reviewing security of said data processing devices comprises the step of reviewing security of data processing devices accessed by users outside of said perimeter.

12. (previously presented) The method as set forth in claim 1, wherein the reviewing security of data processing devices that transfer data across the perimeter of the network comprises categorizing components as either control points or non-control points.

13. (previously presented) The method as set forth in claim 12, wherein the reviewing vulnerability of applications or data processing devices within said perimeter from computers or users outside of said perimeter comprises:

testing control points with port scans; and

testing control points with penetration tests.

14. (previously presented) The method as set forth in claim 1, further comprising:

performing a policy review of an enterprise which owns or controls said network;

defining review parameters based upon the policy review; and

utilizing the review parameters to perform each of: the reviewing security of a network perimeter architecture, the reviewing security of data processing devices that transfer data across the perimeter of the network, the reviewing security of applications that transfer data across said

perimeter, and the reviewing vulnerability of applications or data processing devices within said perimeter from computers or users outside of said perimeter.

15. (previously presented) The method as set forth in claim 1, wherein:

the reviewing security of a network perimeter architecture comprises receiving review parameters from a policy review and generating test cases;

the reviewing security of data processing devices that transfer data across the perimeter of the network comprises receiving the review parameters, receiving the test cases, and performing the test cases;

the reviewing security of applications that transfer data across said perimeter comprises receiving the review parameters, receiving the test cases, and performing the test cases; and

the reviewing vulnerability of applications or data processing devices within said perimeter from computers or users outside of said perimeter comprises receiving the review parameters, receiving the test cases, and performing the test cases.

16. (previously presented) A computer program product comprising a computer usable medium having a computer readable program embodied in the medium, wherein the computer readable program when executed on a computing device is operable to cause the computing device to:

review security of a network perimeter architecture;

review security of data processing devices that transfer data across the perimeter of the network;

review security of applications that transfer data across said perimeter;

review vulnerability of applications or data processing devices within said perimeter from computers or users outside of said perimeter; and

generate a report concerning security of said perimeter based upon all said reviews.

17. (previously presented) The computer program product of claim 16, wherein each of the reviewing security of a network perimeter architecture, the reviewing security of data processing devices that transfer data across the perimeter of the network, the reviewing security of applications that transfer data across said perimeter, and the reviewing vulnerability of applications or data processing devices within said perimeter from computers or users outside of said perimeter utilize review parameters defined in a policy review of an enterprise which owns or controls said network.

18. (previously presented) A system, comprising:

a network having a perimeter; and

a terminal connected to the network and arranged to:

review security of a network perimeter architecture;

review security of data processing devices that transfer data across the perimeter of the network;

review security of applications that transfer data across said perimeter;

review vulnerability of applications or data processing devices within said perimeter from computers or users outside of said perimeter; and

generate a report concerning security of said perimeter based upon all said reviews.

19. (previously presented) The system of claim 18, wherein the report is based upon data provided by the reviewing security of a network perimeter architecture, the reviewing security of data processing devices that transfer data across the perimeter of the network, the reviewing security of applications that transfer data across said perimeter, and the reviewing vulnerability of applications or data processing devices within said perimeter from computers or users outside of said perimeter

20. (previously presented) The system of claim 18, wherein each of the reviewing security of a network perimeter architecture, the reviewing security of data processing devices that transfer data across the perimeter of the network, the reviewing security of applications that transfer data across said perimeter, and the reviewing vulnerability of applications or data processing devices within said perimeter from computers or users outside of said perimeter utilize review parameters defined in a policy review of an enterprise which owns or controls said network.